## I. Rappels

- Switch (niveau 2) : « routage » de trame au niveau des adresses MAC entre ses différents ports
- Routeur (niveau 3) : routage de paquets IP (adosse des domaines de broadcast)

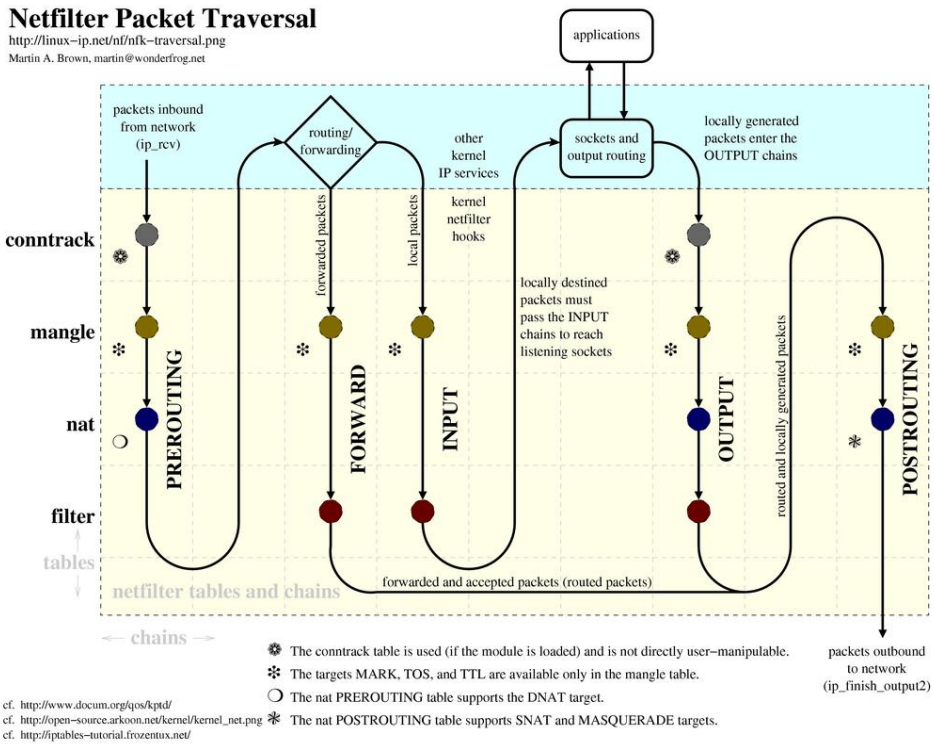
## II. Les VLAN

- VLAN : Réseau isolé de façon virtuelle dans un switch en regroupant certains ports du switch. Pour les trames non taggées, on met un VLAN natif au switch
- 802.1Q :
  - Permet de regrouper plusieurs VLAN sur un lien physique en taggant les paquets avec leur VLAN.
  - Permet de relier 2 switchs entre eux.
- Swtich de niveau 3 :
  - Routage inter-VLAN.
  - Globalement proche d'un routeur.
  - Possède une adresse IP par VLAN.

## III. Les firewalls

- Filtrage des paquets, généralement entre deux réseaux
- Liste de règles + politique par défaut
- Firewall stateless :
  - Ne connait pas l'état de la connexion (ne sait pas si un paquet est une demande ou une réponse)
- Firewall stateful :
  - Conserve une table des connexions pour identifier demandes et réponses

### 1. Schéma iptables



# IV. Network Address Translation

- Le firewall remplace l'adresse source ou destination par la sienne.

# V. IDS (Intrusion Detection System)

## 1. HIDS

- Analyse de log et d'empreinte

## 2. NIDS (Network Intrusion Detection System)

- Analyse du flux réseau pour rechercher des signatures d'attaques
    - Outils de test de sécurité
    - Failles connues (failles génériques, failles applis web, failles logicielles, …)
- Analyse statistique du réseau
- Problèmes : liens trop gros, attaques trop fréquentes, flux chiffrés, exploitation trop chère

# VI. IPS (Intrusion Prevention System)

- Firewall de couche 7 qui bloque en cas d'attaque

# VII. Proxy

- Intermédiaire entre internet et les clients.
- Reverse proxy : renvoi des communications entrantes vers une ou plusieurs machines du réseau privé.